UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/820,682	04/08/2004	Ziv Haparnas	1005-11-01 USP	8531

42698 7590 03/12/2009

CENTURY IP GROUP, INC. [Main]
P.O. BOX 7333
NEWPORT BEACH, CA 92658-7333

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
03/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/820,682	HAPARNAS, ZIV	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-6,8 and 16-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4-6,8 and 16-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This final action is in response to the amendment filed on 10/16/2008. Claims 1, 2, 4-6, 8, & 16-21 are pending and have been considered as follows.

Examiner Note

In light of the applicant's remarks and amendments, the examiner hereby withdraws his previous Specification Objections with respect to the subject matter in Claims 1 & 16, withdraws his previous Claim Objections with respect to Claims 1 & 11, withdraws his previous 35 U.S.C. 101 rejection with respect to Claim 16, withdraws his previous 35 U.S.C. 112 1st paragraph rejections with respect to Claims 1 & 16, and withdraws his previous 35 U.S.C. 112 2nd paragraph rejection with respect to Claim 16.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1, 2, 16, & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorklund et al. (US-5539824-A) in view of Trossen (US-20050021976-A1).

Claims 1 & 16:

Bjorklund et al. disclose a method implemented by a server system/a system configure to secure communications between a service provider and a mobile device in a mobile communications network comprising,

- "receiving a request from the mobile device to provide a unique security key" (i.e. "Actually the considered remote station RS user runs a program provided with the adapter, conventionally referred to as the diagnostics program…The network manager searches into its stored data, for an already installed base (in present implementation that would relate to the first or any already installed and still active network base), and provide it with the received mobile station UA address and name information") [column 4 lines 25-27, 31-36];
- "generating a unique security key, in response to receiving the request from the mobile device" (i.e. "The first base adapter also generates a new name parameter, so-called name', by using a predefined logic function using the parameters Knet(name), UA and Km (step 20), then sends name' to the mobile remote station adapter (step 21)") [column 4 lines 42-46];
- "storing the unique security key in association with an identifier of the mobile device in a first data storage mechanism in the server system" (i.e. "The network manager searches into its stored data") [column 4 lines 31-32];

- "providing the unique security key to the mobile device" (i.e. "The mobile remote station knowing the logic function applied in the corresponding base station, extracts Knet(name) from name' (step 22)") [column 4 lines 49-52];
- "wherein the mobile device stores the unique security key in a second data storage mechanism in the mobile device" (i.e. "stores it (step 23) safely in some protected memory") [column 4 lines 49-52];
- "receiving a request from the service provider to provide the unique security key" (i.e. "It is performed between a remote station adapter and its corresponding base station adapter, then between the base station and the wireless manager or more generally speaking the network manager (WM)") [column 3 lines 46-49];
- "wherein the service provider requests the unique security key in order to establish a secure communication session with the mobile device" (i.e. "It is performed between a remote station adapter and its corresponding base station adapter, then between the base station and the wireless manager or more generally speaking the network manager (WM)") [column 3 lines 46-49];
- "wherein the secure communication session is established between the service provider and the mobile device, in response to the service provider presenting the unique security key to the mobile device for authentication" (i.e. "reliably authenticate the exchange of messages between communicating parties. This involves the establishment of a session key, which key needs being distributed safely") [column 1 lines 44-48];

but, they do not explicitly disclose,

- "providing the unique security key to the service provider, in response to determining that the service provider is included in a list of approved service providers," although Trossen does suggest verification of an authorization prior to providing access, as recited below;
- "wherein the list of approved service providers is updatable by the mobile device," although Trossen does suggest maintaining an authorization associated with an access control, as recited below;

however, Trossen does disclose,

- "the event server can accept the subscription message if the authorization is verified to thereby provide the second network entity with access to the event" [page 2 para 10 lines 5-8];
- "Upon granting consent and receiving, confirming and/or modifying the parameters of the authorization, the software application can automatically create the authorization" [page 4 para 33 lines 1-4];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "providing the unique security key to the service provider, in response to determining that the service provider is included in a list of approved service providers" and "wherein the list of approved service providers is updatable by the mobile device," in the invention as disclosed by Bjorklund et al. for the purposes of providing an access control list to determine communications access.

Claims 2 & 17:

Bjorklund et al. and Trossen disclose a method implemented by a server system/a system configure to secure communications between a service provider and a mobile device in a mobile communications network, as in Claims 1 & 16 above, but, they do not explicitly disclose,

- "wherein the list of approved service providers is stored in at least one of the first and second data storage mechanisms," although Trossen does suggest creating an authorization, as recited below;

however, Trossen does disclose,

- "The authorization can be created in any number of manners, but typically comprises an electronic file that authorizes the requester 18 to access the requested event-based information available from the resource 16 of the user device 12 based upon the parameters included in the authorization" [page 4 para 33 lines 4-9];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the list of approved service providers is stored in at least one of the first and second data storage mechanisms," in the invention as disclosed by Bjorklund et al. for the purposes of providing an access control list to determine communications access.

3. Claims 4 & 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorklund et al. (US-5539824-A) in view of Trossen (US-20050021976-A1) in view of Hind et al. (US-6980660-B1).

Claims 4 & 8:

Bjorklund et al. and Trossen disclose a method implemented by a server system/a system configure to secure communications between a service provider and a mobile device in a mobile communications network, as in Claims 1 & 16 above, but, their combination do not explicitly disclose,

- "the second data storage mechanism is a memory chip embedded in the mobile device," although Hind et al. does suggest a smartcard chip, as recited below;

however, Hind et al. do disclose,

- "smartcard chip" [column 8 line 36];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second data storage mechanism is a memory chip embedded in the mobile device," in the invention as disclosed by Bjorklund et al. and Trossen since it is reasonable to expect the mobile device to have memory for the purposes of storing information.

4. Claims 5, 6, 8 & 19-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bjorklund et al. (US-5539824-A) in view of Trossen (US-20050021976-A1) in view of Ketcham (US-6075860-A).

Claims 5, 6, 19, & 20:

Bjorklund et al. and Trossen disclose a method implemented by a server system/a system configure to secure communications between a service provider and a mobile device in a mobile communications network, as in Claims 1 & 16 above, but, their combination do not explicitly disclose,

- "the second data storage mechanism is an identity module removably insertable in the mobile device," although Ketcham does suggest an authentication that is insertable and removable, as recited below;
- "the second data storage mechanism is a SIM card for the mobile device," although Ketcham does suggest a GSM SIM, as recited below;

however, Ketcham do disclose,

- "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences" [column 8 lines 13-18];
- "authentication card 118 takes the form of a GSM subscriber identity module (SIM)" [column 8 lines 21-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the second data storage mechanism is an identity module removably insertable in the mobile device" and "the second data storage mechanism is a SIM card for the mobile device," in the invention as disclosed by Bjorklund et al. and Trossen for the purposes of providing a removable/insertable authentication card similar to a "smart card" as found in a mobile device for the purposes of storing an embedded identifier used in authentication.

Claims 8 & 21:

Bjorklund et al. and Trossen disclose a method implemented by a server system/a system configure to secure communications between a service provider and a mobile device in a mobile communications network, as in Claims 1 & 16 above, but, their combination do not explicitly disclose,

- "the identifier is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) or a phone number," although Ketcham does suggest utilizing a stored mobile subscriber identity or some other form of unique identity, as recited below;

however, Ketcham do disclose,

- "Authentication card 118 stores an MSID 204, an authentication encryption key 206, and optionally may store other information such as algorithmic identifiers 402, optional parameters 412 for configuring or personalizing a remote terminal 102 according to an authorized user's preferences" [column 8 lines 13-18];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the identifier is at least one of the mobile device's electronic serial number (ESN), international mobile equipment identity (IMEI) or a phone number," in the invention as disclosed by Bjorklund et al. and Trossen for the purposes of providing a unique identifier used in authentication.

Response to Arguments

5. Applicant's arguments with respect to claims 1, 2, 4-6, 8, & 16-21 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

Conclusion

6. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2400 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
03/11/2009

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436